3GPP TSG SA WG3 Security **S3-030245**

6th – 9th May, 2003

Berlin, Germany

Agenda Item:	7.19 Presence
Source:	Ericsson
Title:	HTTP Security in Mt interface
Document for:	Discussion/Decision

1. Introduction

This document discusses security solutions for IMS/Presence Mt interface. The solution based on HTTP Digest AKAv2 is further developed, and comments from SA3 are requested.

2. Alternative solutions

SA3#27 agreed on the following working assumption related to HTTP security:

- TLS is the preferred mechanism for protecting the Mt interface
- Authentication solution should be based on the re-use of AKA
- Interleaving attack related to some scenarios should be further analyzed and eliminated

Ericsson, Nokia and Siemens have presented several alternative solutions that are based on TLS and the re-use of AKA (see examples in Table 1).

Solution	**Referred to in**
1) Re-use of IMS registration	S3-030056 (Siemens)
2) Bootstrapped short-lived subscriber certificates	S3-030060 (Nokia)
3) Bootstrapped HTTP Digest	S3-030060 (Nokia) S3-030056 (Siemens)
4) Combined HTTP Digest AKA & HTTP Digest	S3-030060 (Nokia)
5) HTTP Digest AKAv2	S3-030069 (Ericsson) S3-030084 (Ericsson) S3-030060 (Nokia)

Table 1: Alternative solutions

Ericsson has evaluated the proposed alternatives and would like to state the following on them:

- HTTP Digest AKA versus Subscriber certificates: Since there will most likely be Mobile Operators that would only like to use AKA in Mt interface, it is not realistic to assume that the solution could be based only on subscriber certificates. For this reason, the starting point for solution 2) in Table 1 should be that subscriber certificates can only be an optional solution for Mt interface.
- Communication with HSS: All other solutions except 1) need to solve the problems related to communicating with HSS. This problem can be solved by introducing a new 'Cx-like' interface either directly between the Application Server or via the 'bootstrapping function'. On the other hand, if the new ‘Cx-like’ interface is not created, the solution is automatically limited to IMS access and does not solve the more general problem of allowing the re-use of AKA for communicating with Application Servers.

- Architecture: All proposed solutions include many architectural issues that are not in the responsibility of SA3. Furthermore, the proposed solutions differ in the degree of interdependencies with other organizations (e.g. IETF), other work items (e.g. subscriber certificates), and other systems (e.g. IMS). Ericsson believes that security is one of the criteria when the final solution is chosen. There are still other important criteria such as architecture, time frame, scope of the solution and re-usability will also play an important role in the end.

3. HTTP Digest AKAv2

Ericsson currently believes that HTTP Digest AKAv2 used with TLS will provide the smoothest migration path from current IMS security to more general re-use of AKA with Application Servers. This approach does not include interdependences to other work items (such as subscriber certificates), and is also able to solve the more general problem than just providing access to one Application Server (what is the case with IMS specific solution). For these reasons, Ericsson has started the process of solving the “interleaving attack” related to HTTP Digest AKAv1 in IETF.

Ericsson has already documented the solution in an Internet-Draft (see attached document), and intends to submit it to IETF soon after finishing the discussions with some IETF experts. The current version is based on the following principles:

1) The solution registers a new HTTP Digest AKA algorithm version.

2) The solution does not change AKAv1 in any other way except that the password used in HTTP Digest is (RES||IK||CK) instead of (RES).

There would have been other ways of solving the problem such as trying to re-use the “service specific data” parameter in the AKAv1 or building additional features to control the authenticator as suggested in [S3-030084] for example. However, the chosen solution introduces no changes to the existing HTTP Digest AKA framework, and is assumed to be accepted by IETF in a relatively short time frame.

Registration of new HTTP Digest AKA algorithm versions could be issued by IANA based on Expert Review. However, IANA will quite often want to know the opinion of the WG related to the IANA registry if that WG is still active in IETF. In the case of HTTP Digest AKA, the relevant IETF WG, i.e. SIP or SIPPING, is still active.

SA3 is asked to analyze the proposed solution in the attached document. In particular, SA3 is asked to review section “5.2 Session Protection”, and evaluate if the use of both IK and CK as the HTTP Digest password is appropriate. Alternatively, the passwords could include only one of the session keys just in case some attacker is able to break the HTTP Digest authentication algorithm in the future. In this case, the remaining session key could still be used to protect the traffic.

4. Solution

Solution is based on architecture originally presented by Nokia in SA3#25 in [S3-020528]. HTTP traffic between the UE and Application Server (or an Authentication Proxy) is protected using TLS server side authentication. HTTP Digest AKAv2 is used to authenticate the UE. A new ‘Cx-like’ interface is needed between Application Server (or Proxy) and HSS. Figure 1 demonstrates how the architecture related to HTTP Digest AKAv2 solution would look like in 3GPP Presence Mt interface. It is assumed that the new Cx-like interface is relatively easy to be developed since many details can be directly copied from IMS/Cx. Note also that if a Proxy performs the authentication (instead of an Application Server), it may be possible to access several Application Servers in the Home Network using the same underlying security.

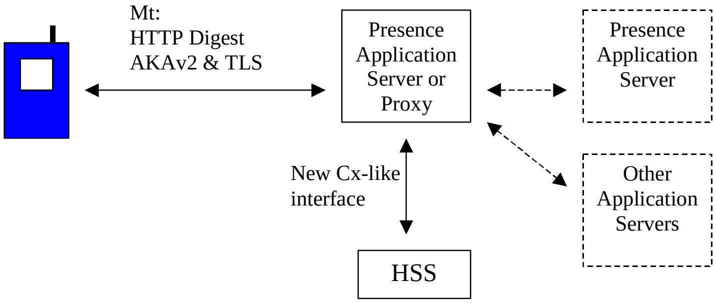
Mt:
HTTP Digest
AKAv2 & TLS
Presence Application Server or Proxy
Presence Application Server
Other Application Servers
New Cx-like interface
HSS

Figure 1: Architecture with HTTP Digest AKAv2 and TLS

5. Conclusions

Ericsson has continued the work related to HTTP Digest AKAv2 and TLS based solution for Mt interface. It is perceived that this solution provides the best migration path from current IMS security to more general re-use of AKA with Application Servers. SA3 is asked to provide comments and feedback for this solution, and the work done in IETF on HTTP Digest AKAv2 (see attached document).

The proposed solution is able to provide access security to several Application Servers as proposed by SA2 in [S3-030193]. The solution is also independent of IMS registration. The dependency of AKAv2 specification work with IETF is not seen as a big risk since AKAv2 is not a new protocol but an extension to an existing one.

Ericsson is not aware of any negative impacts that would be related to the use of proxy in the Mt interface as asked by SA2 in [S3-030210].

SA3 should consider sending liaison statement to CN4 and SA2 on potential new Cx-like interface if AKA is re-used for Mt interface.

6. References

[S3-020528] Nokia (2002) HTTP Security, 3GPP, SA3#25, 8 - 11 October, Munich, Germany.

[S3-030056] Siemens (2003) Security solution for IMS-related HTTP services, 3GPP, S3#26, 25 - 28 February, Sophia Antipolis, France.

[S3-030060] Nokia (2003) HTTP authentication, 3GPP, S3#26, 25 - 28 February, Sophia Antipolis, France.

[S3-030069] Ericsson (2003) The use of HTTP in Presence/IMS, 3GPP, S3#26, 25 - 28 February, Sophia Antipolis, France.

[S3-030084] Ericsson (2003) How to mitigate the Interleaving attack and reduce the trust in the Authenticator, 3GPP, S3#26, 25 - 28 February, Sophia Antipolis, France.

[S3-030193] 3GPP SA2 WG (2003) LS on enhancements of the Mt reference point, S2-031561.

[S3-030210] 3GPP SA2 WG (2003) Response to LS (S2-030445) on use of HTTP between UE and AS in the IMS, S2-031583.

SIPPING Working Group
Internet-Draft
Expires: October 29, 2003

V. Torvinen
J. Arkko
Ericsson

April 30, 2003

Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2
Draft-torvinen-sipping-digest-aka-v2-00.txt

Status of this Memo

Copyright Notice

Abstract

HTTP Digest is known to be vulnerable to man-in-the-middle attacks, even when run inside TLS, if the same passwords are used for authentication in some other context without TLS. This is a general problem that affects not just HTTP digest but also other IETF protocols. However, for a class of strong algorithms the attack is avoidable. This document defines version 2 of the HTTP Digest AKA algorithm. Unlike previous versions of HTTP Digest such as MD5 or AKAv1, this algorithm is immune to the man-in-the-middle attack.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

The Hypertext Transfer Protocol (HTTP) Digest Authentication, described in [RFC2617], has been extended in [RFC3310] to support Authentication and Key Agreement (AKA) mechanism [AKA-REF]. AKA mechanism performs authentication and session key distribution in Universal Mobile Telecommunications System (UMTS) networks. HTTP Digest AKA enables the usage of AKA as a one-time password generation mechanism for Digest authentication.

HTTP Digest is known to be vulnerable to man-in-the-middle attacks, even when run inside TLS, if the same HTTP Digest authentication credentials are used in some other context without TLS. The attacker may initiate a TLS session with a server, and when the server challenges the attacker with HTTP Digest, the attacker masquerades the server to the victim. If the victim responds to the challenge, the attacker is able to use this response towards the server in HTTP Digest. Note that this attack is an instance of general attack that affects a number of IETF protocols such as PIC. The general problem is discussed in [Asokan-Niemi-Nyberg] and [Puthenkulam-binding-draft].

Because of the previous vulnerability, the use of HTTP Digest "AKAv1" should be limited to the situations where the client is able to demonstrate that in addition to AKA response, it possess the AKA session keys. This is possible, for example, if the underlying security protocol uses the AKA generated session keys to protect the authentication response. This is the case for example in the 3GPP IP Multimedia Core Network Subsystem (IMS) where HTTP Digest "AKAv1" is currently applied. However, HTTP Digest "AKAv1" should not be used with tunnelled security protocols that do not utilize the AKA session keys. For example, the use of HTTP Digest "AKAv1" is not necessarily secure with TLS if the server side is authenticated using certificates and the client side is authenticated using HTTP Digest AKA.

There are at least four potential solutions to the problem:

1. The use of the authentication credentials is limited to one application only. However, this would increase the total number of authentication credentials for an end-user, and would cause scalability problems in the server side.

2. The keys used in the underlying security protocols are somehow bind to the keys used in the tunneled authentication protocol. However, this would cause problems with the current implementations of underlying security protocols. For example, it is not possible to use the session keys from TLS at application

layer. Furthermore, this solution would only solve the problem when HTTP Digest is used over one hop, and leave the problem of using HTTP Digest via multiple hops, e.g. via proxy servers, unsolved.

3. Authentication credentials are used in cryptographically different way for each media and/or access network. However, it may be difficult to know which underlying media is used below the application.

4. Authentication credentials are used in cryptographically different way for each application.

This document specifies a new algorithm version for HTTP Digest AKA, i.e. "AKAv2". "AKAv2" specifies a cryptographically different way to use AKA credentials in applications that are based either on HTTP Digest authentication or UMTS authentication (cf. approach 4 above). The only difference to "AKAv1" is that in addition to AKA response RES the AKA related session keys, IK and CK, are also used as the password for HTTP Digest. AKAv2 is immune to man-in-the-middle attack described above. However, if AKAv2 is used in some environment both with and without some underlying security, such as TLS, the problem still exists.

New HTTP Digest AKA algorithm versions can be registered in IANA based on Expert Review. Documentation of new algorithm versions is not mandated as RFCs. However, "AKAv2" is documented as an RFC because the use of different AKA algorithm versions includes security implications that the implementators should be aware of. The extension version and security implications are presented in this document.

2.1 Terminology

This chapter explains the terminology used in this document.

AKA

Authentication and Key Agreement.

AKA is a challenge-response based mechanism that uses symmetric cryptography. AKA can be run in a UMTS IM Services Identity Module (ISIM) or in UMTS Subscriber Identity Module (USIM), which reside on a smart card like device that also provides tamper resistant storage of shared secrets.

CK

Cipher Key. An AKA session key for encryption.

IK

Integrity Key. An AKA session key for integrity check.

ISIM

IP Multimedia Services Identity Module. Sometimes ISIM is implemented using USIM.

RES

Authentication Response. Generated by the ISIM.

SIM

Subscriber Identity Module. GSM counter part for ISIM and USIM.

UMTS

Universal Mobile Telecommunications System.

USIM

UMTS Subscriber Identity Module. UMTS counter part for ISIM and SIM.

XRES

Expected Authentication Response. In a successful authentication this is equal to RES.

3. Digest password generation in AKAv2

In general, the Digest AKAv2 operation is identical to the Digest AKAv1 operation described in [RFC3310]. This chapter specifies the parts in which Digest AKAv2 is different from Digest AKAv1 operation. The notation used in the Augmented BNF definitions for the new and modified syntax elements in this section is as used in SIP [RFC3261], and any elements not defined in this section are as defined in [RFC3310].

In order to direct the client into using AKAv2 for authentication instead of other AKA versions or other HTTP Digest algorithms, the AKA version directive of [RFC3310] shall have the following new value:

```
aka-version         =  "AKAv2"
```

The AKA version directive is used as a part of the algorithm field as defined in [RFC3310].

```
Example:  algorithm=AKAv2-MD5
```

The client shall use the concatenated AKA parameters (RES||IK||CK) as a "password" when calculating the HTTP Digest response directive for AKAv2.

The server shall use the concatenated AKA parameters (XRES||IK||CK) as a "password" when checking the HTTP Digest response or when calculating the "response-auth" of the "Authentication-Info" header.

4. Example Digest AKAv2 Operation

This document does not introduce any changes to the operations of HTTP Digest or HTTP Digest AKA. Examples defined in [RFC3310] applies directly to AKAv2 with the following two exceptions:

1. The algorithm directive has a prefix "AKAv2" instead of "AKAv1".

2. The HTTP Digest password is derived from (RES||IK||CK) or (XRES||IK||CK) instead of (RES) or (XRES) respectively.

5. Security Considerations

5.1 Multiple Authentication Schemes and Algorithms

The rules for an user agent for choosing among multiple authentication schemes and algorithms are as defined in [RFC3310] except that the user agent MUST choose "AKAv2" if both "AKAv1" and "AKAv2" are present.

Since HTTP Digest is known to be vulnerable for bidding-down attack in environments where multiple authentication schemes and/or algorithms are used, the system implementators should pay special attention for scenarios where both "AKAv1" and "AKAv2" are used. Especially if the AKA generated sessions keys or some other additional security measures to authenticate the clients, such as client certificates, are not used, the use of both AKA algorithm versions should be avoided.

5.2 Session Protection

Even though "AKAv2" uses the additional integrity (IK) and confidentiality (CK) keys as a part of HTTP Digest AKA password, these session keys may still be used for creating additional security within HTTP authentication or some other security mechanism. This recommendation is based on the assumption that algorithms used in HTTP Digest, such as MD5, are sufficiently strong one-way functions, and consequently HTTP Digest responses leak no or very little computational information about IK and CK.

5.3 Man-in-the-middle attacks

[Asokan-Niemi-Nyberg] describe a "man-in-the-middle" attack related to tunnelled authentication protocols. [Asokan-Niemi-Nyberg] discuss the attack mostly in EAP context; however, it can exist in any similar contexts where tunnelled authentication is used and where the same authentication credentials are used without protection in some other context or the client fails to authenticate the server.

For example, the use of TLS with HTTP Digest authentication (i.e. TLS for server authentication, and subsequent use of HTTP Digest for client authentication) is an instance of such scenario. HTTP challenges and responses can be fetched from and to different TLS tunnels without noticing where they originally came from. Especially, the attack is easy to perform if the client fails to authenticate the server. If the same HTTP credentials are used with unsecured connection, the attack is also easy to perform.

This is how the "man-in-the-middle" attack works with HTTP Digest and

TLS if the victim (i.e. the client) fails to authenticate the server:

1. The victim contacts the attacker using TLS. If the attacker has a valid server certificate, the client may continue talking to the

attacker and use some HTTP authentication compatible protocol, such as Session Initiation Protocol (SIP).

2. The attacker contacts some real proxy/server also using TLS and some HTTP authentication compatible protocol. The proxy/server responds to the attacker with HTTP Authentication challenge.

3. The attacker forwards the HTTP Authentication challenge from the proxy/server to the victim. If the victim is not careful, and check that the identity in the server certificate in TLS matches the realm in the HTTP authentication challenge, it may send a new request which carries a valid response to the HTTP Authentication challenge.

4. The attacker may use the response with the victims HTTP Digest username and password to authenticate itself to the proxy/server.

The man-in-the-middle attack is not possible if the client compares the identities in the TLS server certificate and the HTTP Digest authentication challenge. Note that with HTTP Basic, the client would send the password to the attacker.

Another variant of the "man-in-the-middle" attack is the so-called "interleaving attack". This attack is possible if the HTTP Digest authentication credentials are used in several contexts, and in one of them without protection.

This is how the attack could proceed:

1. The attacker establishes a TLS tunnel to the proxy/server using one-way server authentication. The attacker sends a request to the proxy/server.

2. The proxy/server challenges the attacker with HTTP Digest challenge.

3. The attacker challenges the victim in some other context using the challenge carried in the HTTP Digest challenge. The HTTP Digest challenge need to be modified to the format used in the protocol of this other context.

4. The victim responds with a response.

5. The attacker uses the response from the other context for

authentication in HTTP Digest.

6. The proxy/server accepts the response, and delivers the service to the attacker.

In some circumstances, HTTP Digest AKAv1 may be vulnerable for the interleaving attack. In particular, if ISIM is implemented using USIM the HTTP Digest AKAv1 should not be used with tunneled security protocols unless the AKA related session keys, IK and CK, are somehow used with the solution.

HTTP Digest AKAv2 is not vulnerable for interleaving attack.

5.4 Entropy

AKAv1 passwords should only be used as one-time passwords if the entropy of the used RES value is limited (e.g., only 32 bits). For this reason, the reuse of the same RES value in authenticating subsequent requests and responses is not recommended. Furthermore, algorithms such as "MD5-sess", which limit the amount of material hashed with a single key, by producing a session key for authentication, should not be used with AKAv1.

Passwords generated using AKAv2 can more securely be used for authenticating subsequent requests and responses because the concatenation of AKA credentials (i.e. RES||IK||CK) makes the passwords significantly longer. The user agent does not need to assume that AKAv2 passwords are limited to one-time use only, and it may try to re-use the AKAv2 passwords with the server. However, the length of the RES still matters because the attacker may try to use pre-calculated dictionaries to guess the (RES||IK||CK). The longer the RES is, the more difficult it is for the attacker to guess the (RES||IK||CK).

6. IANA Considerations

This document specifies a new aka-version, "AKAv2", to the aka-version namespace maintained by IANA. The allocation of new aka-versions is up to Expert Review as outlined in [RFC2434].

6.1 Registration Information

To: ietf-digest-aka@iana.org

Subject: Registration of a new AKA version

Version identifier: "AKAv2"

Contacts for further information: vesa.torvinen@ericsson.fi or jari.arkko@ericsson.com

Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3310] Niemi, A., Arkko, J. and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

Informative References

[AKA-REF] 3rd Generation Partnership Project, "Security Architecture (Release 4)", TS 33.102, December 2001.

[Asokan-Niemi-Nyberg]
Asokan, N., Niemi, V. and K. Nyberg, "Man-in-the-Middle in Tunnelled Authentication Protocols", Cryptology ePrint Archive, http://eprint.iacr.org Report 2002/163, October 2002.

[Puthenkulam-binding-draft]
Puthenkulam, J., Lortz, V., Palekar, A. and D. Simon, "The Compound Authentication Binding Problem", IETF, Work in progress draft-puthenkulam-eap-binding-02.txt, March 2003.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

Authors' Addresses

Vesa Torvinen
Ericsson
Joukahaisenkatu 1
Turku FIN 20520
Finland

Phone: +358 40 7230822
EMail: vesa.torvinen@ericsson.fi

Jari Arkko
Ericsson
Hirsalantie 1
Jorvas FIN 02420
Finland

Phone: +358 40 5079256
EMail: jari.arkko@ericsson.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.